BUMIS
Bureau of Medicine and Surgery Information System

Questions or comments related to this plan should be directed to:

Contingency Plan Point of Contact:
Mr. Anthony Long
Naval Medical Information Management Center
301-319-1120
aflong@us.med.navy.mil

BUMIS II

Continuity of Operations Plan

Ensuring System Operations For the Next Century

Prepared by:
Anthony F. Long
Program Manager
Naval Medical Information
Management Center (NMIMC)

1.0 INTRODUCTION

The Year 2000 (Y2K) problem poses an enormous management and technical challenge to systems worldwide. Careful planning and execution will enable systems to identify and resolve their Y2K problems prior to fiscal year 1999. The Resource Business Area (RBA), in accordance with the Department of Defense (DOD) and the Military Health System (MHS) guidance, has identified specific activities needed by all Automated Information Systems (AIS) in the identification and resolution of potential Y2K problems. To mitigate the potential risk caused by Y2K problems, all AISs have been directed to provide a Y2K contingency plan. The plan should include instructions for implementing the contingency plan, procedures for operating in a contingency mode, and guidance for returning to normal operating procedures.

In an effort to assess and manage its Y2K risk, MHS categorized all AIS based on their functions in support of the MHS mission. The categorizations are mission critical, mission essential, and mission support. Mission critical systems are defined as those systems in which the loss of their critical functions would cause *immediate* stoppage of the direct medical mission (including force protection, direct patient care and safety). Mission essential systems are defined as those systems in which the loss of their functions would *reduce* medical mission. If not corrected promptly, significant medical mission impact will result. The Bureau of Medicine and Surgery Information System II (BUMIS II) is categorized as a mission essential system.

BUMIS II is a personnel management system. Date calculations are used for personnel management issues such as projecting future losses and determining what specialties will be available to support mission requirements at particular activities. Date calculations are also used to correct non-Y2K Compliant information received from other sources, such as BUPERS. The impact of non-Y2K Compliance would be inaccurate information being supplied to decision makers, and problems generating reports needed for Medical Department Officers' Special Pays. Also, the Medical Department would be unable to properly staff its officer billets, since the BUMIS II system provides the information necessary to project needs and schedule the rotation of officers.

1.1 OBJECTIVES

The objective of this plan is to outline a strategy for continued operational support in the event that BUMIS II fails on, near, or after the Year 2000. In addition, this plan assesses the potential Y2K risk, its impact to the program, and identifies alternative procedures. This plan serves as a guide to the BUMIS II Project Manager allowing them to:

- Establish, organize, and document risk assessments, responsibilities, policies, and procedures
- Identify potential risk and ensure that adequate preparations have been made to continue the BUMIS II mission support operations
- Streamline decision-making during the contingency situations
- Identify and implement procedures to ensure continued operations

- Ensure resumption of failed mission operations at the earliest possible time, in the most cost-effective manner

Approved contingency plans and Continuity of Operations Plans (COOP) are mandatory to obtain MHS AIS certification. Appropriate personnel must be identified and trained to implement contingency procedures, and the plans must be tested and updated periodically to ensure that they are valid and current. Relevant contingency information should be exchanged between medical facility commanders, business area managers, project managers, and external organizations to ensure that users of BUMIS II and its interfacing systems are aware of alternative mission support procedures.

1.2 BACKGROUND

BUMIS II is a client-server program that provides headquarters users with the ability to mange the personnel information of Medical Corps, Dental Corps, Medical Service Corps, and Nurse Corps officers. This information is used to project personnel needs in specific specialties, provide information related to the availability of officers with critically needed skills, and respond to requirements levied by higher authorities. Without the BUMIS II system in operation, the ability of the Medical Department to staff officer billets is severely impaired.

BUMIS II contains information that is specific to the BUMED Officer Corps. This information is merged with data from BUPERS to provide a complete description of these officers.

BUMIS II replaced the legacy BUMIS I system, which was a mainframe application using character-based terminals.

1.3 SYSTEM ARCHITECTURE

BUMIS II is a client-server system. The minimum server configuration recommended is a Dual-Pentium II 266, 256 MB RAM, 8 GB HD, Microsoft Windows NT Server Version 4.0 SP3 or higher, Microsoft SQL Server 6.5 SP3 or higher, and 10/100BaseT network card. The minimum system configuration recommended for a workstation is a Pentium 166, 64 MB RAM, 1 GB HD, Microsoft Windows NT Workstation 4.0 SP3 or higher, Microsoft Access 97 w/SR1 or higher, and a 10/100BaseT network card. The BUMIS II Program Office is not responsible for supplying workstations. However, the primary users of the system at BUMED Headquarters have all been upgraded to systems that exceed these requirements.

BUMIS II depends on reliable TCP/IP networking between the server and clients. The primary system users are at BUMED Headquarters in Washington, DC, and the Naval Medical Information Management Command (NMIMC) in Bethesda, Maryland. These two facilities are connected by a dedicated T-1 line.

The BUMIS II information is stored in a SQL Server database. The client is written in Microsoft Access 97. Database connectivity is based on Object DataBase Connectivity (ODBC) drivers supplied by Microsoft.

1.3 ROLES AND RESPONSIBILITIES

The following organizations or managers have roles and responsibilities associated with BUMIS II Y2K contingency and continuity of operations planning:

Resource Business Area

- Review and approve BUMIS II contingency plans and COOPs
- Forward approved contingency plans and COOPS to OASD(HA) for review. Oversee efforts for BUMIS II internal and external interface agreements (including testing and the development of procedures to ensure the continued exchange of mission data between business area functions)
- Oversee business area operational end-to-end testing including exercising and testing continuity of operations plans
- Oversee business area operational test program including internal and external interfaces.

BUMIS II Project Office

- Develop contingency plans and continuity of operations plans
- Document system interfaces and obtain interface agreements for each interface
- Submit plans to business area manager for review and approval
- Test contingency procedures
- Oversee operational testing in a live environment.
- Oversee testing with external interfaces
- Oversee renovation, validation, and implementation of Y2K compliant software.

User Organizations

- Interface with BUMIS II Project Office for acceptance of corrected software or for scheduling on-site implementation of software fixes or fixes related to hardware, system software, local/wide area communications.
- Test BUMIS II COOP
- Accept, review, tailor BUMIS II Continuity of Operations Plan inputs

- Integrate/append BUMIS II Y2K COOP with existing plans
- Report Y2K suspected problems as defined in the BUMIS II Y2K COOP
- Implement COOP Contingency mode procedures, as required and as directed.

2.0 PROGRAMMATIC ELEMENT CONTINGENCY PLAN

A programmatic risk assessment was conducted using the MHS Y2K Programmatic Risk Assessment Question. The results are shown in figure 2.1 concludes that the programmatic risk to ensure total system compliance within the mandated timelines are low. The Y2K fixes that were needed were minor and did not necessitate additional funding therefore no significant cost or technical risks are perceived. A potential cost risk is that contingency funds have not been identified to cover unanticipated renovation, testing, and/or implementation issues. The Y2K fixes, which are explained in more detail in the section 2.4, were deployed in December 1998. All renovation, testing, and implementation activities will be complete by the mandated timelines.

2.1 PROGRAMMATIC RISK ASSESSMENT

Y2K Programmatic Risk Assessment Questionnaire	
AIS: BUMIS II	**Date: 02/26/1999**
Cost Risk Evaluation	
1. Has the renovation of the system or replacement system been fully funded? ***Yes*** 2. Does the funding include the deployment, testing, implementation, training, and conversion of the new or renovated system? ***Yes, it is fully funded.*** 3. Has the cost of ensuring Y2K compliance of the operating system/executive software and hardware been funded? ***The Operating System and Hardware are Y2K compliant.*** 4. Have all interfaces (internal and external) been identified and has sufficient funding been earmarked to ensure renovation, testing, and certification, as required? ***Yes*** 5. Are contingency funds available to cover unexpected renovation, testing, and/or implementation issues? ***No.*** **Rating:** ***Low Risk***	
Schedule Risk Evaluation	
1. Have all DoD and MHS mandated phase milestones been achieved? * ***No*** 2. Is the implementation going to be achieved within the DoD and MHS mandates? * ***Yes*** 3. Have testing and rework activities been factored into the schedule? ***Yes*** 4. Have interface renovations/development (internal & external) been factored into the schedule? ***Yes*** 5. Has sufficient time been scheduled for interface testing, rework, and certification? ***Yes*** 6. Are there significant schedule interdependencies with other AIS projects? ***No*** 7. Are there significant interdependencies with system s/w, hardware, or infrastructure elements? ***No*** 8. Are COTS vendor schedules adequate to meet DoD and MHS requirements? ***N/A*** 9. Has a master program schedule network been developed in an automated project management tool? ***Yes*** 10. Has a critical path been identified and has critical path analysis been performed? ***Yes*** ***** If the answer question 2 is NO, schedule risk must be classified as "High." **Rating**: ***Low Risk***	

Y2K Programmatic Risk Assessment Questionnaire
Performance/Technical Risk Evaluation
1. Has a formal Y2K Project Plan been prepared, approved, and published? ***Yes*** 2. Does the project plan address system software and system-to-system interfaces? ***Yes*** 3. Does the plan address local area/wide area communications? ***No*** 4. Does the plan address data conversion, testing, training, and certification requirements? ***Yes*** 5. Has the local area communications system (LAN) been determined compliant? ***No*** 6. Does the plan include procedures for ensuring Y2K compliance of system software and hardware been confirmed? ***Yes*** 7. Does the plan call for system-level testing to include COTS products and internal and external interfaces? ***Yes*** **Rating:** ***Low Risk***

Table 2-1. Y2K Programmatic Risk Assessment Questionnaire

2.2 PERFORMANCE/TECHNICAL RISK MANAGEMENT

BUMIS II is written in Microsoft SQL Server 6.5, which has a comprehensive date computation capability and can handle full eight-digit dates. The data imported from the legacy BUMIS I system has been fully converted to eight-digit dates.

The Y2K problem may also cause a problem with expiring software licenses, system passwords, and user accounts. In BUMIS II, these are managed by the Microsoft Windows NT operating system, which is Y2K compliant.

2.3 RISK CONTROLS

As part of the risk assessment, Figure 2-2 has been prepared to document the various technical and cost risks facing the BUMIS II Project Office.

Risk	Risk Mitigation
Performance/Technical Risks	
Performance/Technical Risk 1: BUMIS II Operating System and software are not upgraded to Y2K compliant status.	• The Operating System has had the appropriate Service Packs installed, and has been tested. • The system has been extensively tested to ensure Y2K compatibility.
Performance/Technical Risk 2: Failure of desktops to be Y2K compliant.	• This is being addressed by the local MID • Even if the desktops were not Y2K compliant, the desktop's system date does not have an effect on the BUMIS II Client software. • The desktops can be set to any date such that

	they may continue operation without effecting the BUMIS II Client software.
Performance/Technical Risk 3: Local area communications infrastructure fails to support the system.	• Spare hub has been made available to the primary users. • Separate network could be established to primary users' PCs using this hub and cabling. • Local MID is addressing network concerns.
Cost Risks	
Cost Risk 1: Potential for inadequate funding for extensive re-programming and re-testing.	• Considered very low. The system is already in parallel testing with the original BUMIS I system. • The system has already passed Y2K testing.

Table 2-2. Risk Control Measures

2.4 Y2K PROBLEMS ALREADY IDENTIFIED

Several small problems related to the data imports from the BUMIS I system were identified. These items were reformatted to properly represent 8-digit dates.

2.5 INTERFACE RISK

BUMIS II exchanges data with BUPERS. BUPERS has stated it will not become Y2K compliant.

BUPERS and BUMIS use "windowing" to exchange data. BUMIS II receives data in six-digit format, and translates them to 8-digits for use internally. When data is exported to BUPERS, the dates are translated from BUMIS II's 8-digit date format to the BUPERS six-digit date format.

2.6 PROJECT SCHEDULE

BUMIS II is currently in the System Testing stage. BUMIS II was initially classified as 'Always Compliant". BUMIS II was pushed back to the Renovation stage while fixing two problems that were identified. The release of this fix in December 1998 was a critical milestone. The following is the BUMIS II Y2K project schedule.

Activity Name	Early Start	Early Finish	Days	Actual Start	Actual Finish	% Complete
Start Assessment	6/2/97	8/22/97	60	6/2/97	8/22/97	100
Complete Assessment	8/23/97	8/22/97	0	8/23/97	8/22/97	100
Develop Risk Management/Contingency Plan-System	8/17/98	10/16/98	45	8/17/98	10/16/98	100

Establish Interface Agreements	5/1/98	8/3/98	67	5/1/98	8/3/98	100
Make Software Repairs	5/1/98	11/23/98	136	5/1/98	11/23/98	100
Conduct Development Integration Testing (DIT)	11/23/98	11/29/98	7	11/23/98	11/29/98	100
Conduct System Integration Testing (SIT)	12/1/98	3/25/99	67	12/1/98		78
Update Risk Management/Contingency Plan	9/30/98	3/25/99	45	9/30/98		100
Draft Y2K Test Plan	10/23/98	10/23/98	1	10/23/98	10/23/98	100
Obtain BA Approval of Test Plan	10/26/98	10/26/98	1	10/26/98	10/26/98	100
Conduct Application Testing	1/6/99	2/26/99	36	1/6/99		86
Conduct H/W and OS Testing	1/6/99	2/26/99	36	1/6/99		86
Conduct Interface Testing	1/6/99	2/26/99	36	1/6/99		86
Document and Validate Y2K Test Results	2/22/99	2/26/99	5	2/19/99		20
Complete Project Manager Y2K Certification	3/26/99	3/26/99	1			0
Submit to IMT&R for IV&V Review	3/27/99	3/31/99	5			0
Obtain BA Y2K Certification	3/27/99	3/27/99	1			0
Update Risk Management/Contingency Plan_System	8/7/98	10/16/98	51	8/7/98	10/16/98	100
Complete Renovation	3/26/99	3/25/99	0			0
Develop Archive/Retrieval Procedures	10/15/98	10/22/98	6	10/15/98	10/22/98	100
Develop Continuity of Operations Plan	11/27/98	12/1/98	1	11/27/98	12/1/98	100
Develop Deployment Plan	10/30/98	12/24/98	6	10/30/98	12/24/98	100
Complete Validation	3/29/99	3/28/99	0			0
Complete Deployment	3/28/99	3/28/99	1			0
Obtain HA Y2K Certification	3/28/99	3/28/99	1			0
Complete Implementation	3/29/99	3/28/99	0			0
Y2K Project Complete	3/29/99	3/28/99	0			0

Table 2-3. Year 2000 Project Schedule

3.0 PROGRAMMATIC ZERO-DAY STRATEGIES

The objective of this programmatic zero-day strategy is to ensure that the BUMIS II Project Office is ready to provide responsive management and control of worst-case scenarios immediately before, during, and after the beginning of FY of CY 2000.

BUMIS II Programmatic Zero-Day Strategies	
Planning Element	**Elements of Zero day Strategy**
Staff resource assignments	• Limit leave for project personnel the week before and four weeks after the fiscal and calendar start dates (1 Oct 99 and 1 Jan 2000). • Include similar limited absence clause in written task statements/delivery orders with system developer and support contractor.
General Readiness	• Include in task statement/delivery order for FY99 that the developmental environment will be reserved for repairing and testing Y2K related system failures. • Include language requiring support contractor and developers to devote key technical personnel to Y2K related problem analysis and repair.
Coordination with interfacing organizations	• Ensure interface agreements are in to ensure roles, responsibilities, and resource allocations are defined and understood. • Jointly develop zero day strategies with BUPERS. • Extensively test post-year2000 data transfers.
Open ongoing communications	• Review and test lines/methods of communications with the user community the last week of September 1999 and the last week of December 1999 • Validate POC list in mid September. • Begin issuing Y2K bulletins to user community during September 1999. First issues to advise user community of test scenarios, current POC list, review problem reporting procedures, and other topics deemed appropriate. • Use Y2K bulletins to advise user community how best to respond to Y2K incidents. • Develop and publish multiple avenues for communicating with the BUMIS II Project Office.
Project schedules	• For each major problem event (a system failure that cannot be corrected within 3 to 5 workdays) a task/project name, number, and master schedule will be entered into P3. • An event schedule will be developed and agreed to by all participants (interfacing organizations, contractors, and vendors), and other interested parties.

Table 3-1. BUMIS II Programmatic Zero day Strategies

4.0 SYSTEM ELEMENT CONTINGENCY PLAN

The purpose of the System Element Contingency Plan is ensure that the BUMIS II Project Office is prepared to handle Y2K failures just before, during, or after the change over to the calendar/fiscal year 2000. This plan provides the procedures for identifying, analyzing, correcting, and redistributing repaired software. This plan will be invoked if any of the following types of failures are reported: application failure, interface failure, hardware failure, corrupt data, or any Y2K-related or other system problem reported by a system user.

4.1 SYSTEM-LEVEL RISK ASSESSMENT

A risk assessment was conducted to determine the probability of a risk occurring (P^o) and the consequence (C^o) of that risk should it occur. The risk classification (RC) is determined by multiplying P^o times C^o. The results of this analytical process are documented in Figure 5.1.

System-Level BUMIS II Contingency Plan					
Normal Operating Procedures	**Risk**	**P^o**	**C^o**	**RC**	**Contingency Operations Mode**
Problem Identification					
1. User reports problem by calling local/MTF system administration.	Local help desk unable to resolve.	H	L	M	User implements partial/full contingency operating mode (e.g., manually support business process).
2. System Administrator reports problem to BUMIS II Help Desk.	BUMIS II Help Desk unable to resolve.	L	L	L	User implements manual operating mode pending problem resolution.
Problem Analyses					
1. BUMIS Contractor front-line support resolves problem.	Unable to resolve problem.	L	L	L	Contact developers to resolve problem.
2. BUMIS II developers resolves problem; provides fix guidance to site.	Developers unable to resolve problem in a timely manner.	L	L	L	Re-direct contractor resources and conduct problem analysis.
3. Coordinate non-BUMIS II problems with MID.	Failure of MID to accept problem ownership or co-ownership.	L	L	L	Implement problem escalation procedures in IA Clearly define what constitutes problem ownership/co-ownership in IA.
4. Determine if problem is caused by hardware, system software, or local/wide area communications.	Failure to identify problem cause by BUMIS II PM.	L	M	M	Re-direct resources to halt work on development and conduct problem analysis.
Software Repair/Problem Resolution					
1. BUMIS II Project Office attempts repairs.	Unable to resolve, not a BUMIS II S/W or Interface problem	L	M	M	Exercise joint agreements with interfacing organization/project.
2. BUMIS II Project Office attempts repairs.	Unable to resolve hardware problem	L	M	M	Exercise pre-existing written agreement with hardware vendor to repair problem.
3. BUMIS II Project Office attempts repairs.	Unable to resolve, local/wide area communications problem.	L	M	M	Coordinate with MID.

4.	BUMIS II Project Office attempts repairs.	Unable to resolve, Operating System issue.	L	M	M	Re-direct contractor resources to repair and coordinate with OS vendors.

Table 4-1. BUMIS II System-Level Contingency Plan

4.2 PROBLEM IDENTIFICATION AND ANALYSIS

The following paragraph describes the problem management process that the BUMIS II Project Office will follow when Y2K problems are encountered and reported by the user community.

1. The user will contact the BUMIS II Project Office (B2PO). The User will receive acknowledgement of the problem report. The problem report will be serialized.
2. The B2PO will contact the contractor.
3. The contractor will contact the user to determine if the problem is clearly a non-BUMIS II issue. If it is a non-BUMIS II issue, the local MID will be contacted, and a trouble ticket will be set up with them. The contractor will coordinate with MID and the user until the problem has been resolved. The B2PO will be informed of the problem resolution.
4. For problems that are possibly related to BUMIS II, a specialist will work with the user to define the problem further. If the problem can be resolved remotely, then the user will be notified, as well as the B2PO. If the problem is determined to be a non-BUMIS II item, then the steps detailed in (3) above will be followed.
5. For problems that require a site visit with the user, a support person skilled in troubleshooting the appropriate type of problem will be dispatch (Hardware, Software, Database, etc.). If the problem is solved, then the user and the B2PO will be notified. If the problem is determined to be a non-BUMIS II item, then the steps detailed in (3) above will be followed.
6. For items that require coordination with the hardware manufacturer, then the contractor will contact the manufacturer and arrange for on-site repairs. The B2PO will be notified.

4.3 SYSTEM-LEVEL ZERO DAY STRATEGIES

The objective of the System-Level Zero Day Strategy is to ensure necessary resources are available to identify, report, accept, and correct systems problems (regardless of cause) immediately before, during, and immediately after the fiscal year and calendar year change to year 2000.

BUMIS II System-Level Zero day Strategies	
Planning Element	**Elements of Zero day Strategy**
Accessibility to the project office	• Establish 7 day, 24 hour DSN and commercial numbers to the BUMIS project office (for user community, interfacing organizations, vendors, contractors, and other personnel that may need to contact the project office. • Set up E-Mail pagers and Cell Phones for key Project Office and contractor personnel • Selected user community zero hour testing to ensure data integrity, interface functionality, and system (hardware, system software, local area and wide area communications.
Primary and alternate problem methods	• BUMIS II Project Office will initiate problem identification methods to identify problems encountered by the user community. • Notify user community immediately once a problem has been identified. • Group mailing address blocks will be established and tested prior to 1 OCT 1999. • E-mail and mailing addressing should be provided to the user community as an integral part of the BUMIS II COOP.
Primary and alternate problem analysis methods	• Primary and alternate methods for problem reporting will be established. • Concurrent reporting to the BUMIS II Project Office and BUMED will be suggested. • Guidelines should be developed for problem description and provided to the user community in the Continuity of Operations Plan.
Joint problem analysis	• Interface Agreements has been established with interfacing systems. Language will be added to include joint problem analysis and resolution.
Establishing problem ownership	• Establish procedures with interfacing organizations business rules that include definitions of what constitute problem ownership. This step is necessary to avoid unnecessary delays in problem resolution.
Primary and alternate problem repair methods	• BUMIS II Project Manager will identify all needed resources necessary to repair system problems under worse case scenarios. Alternative methods (and/or supplemental resources will be identified and available for the system-level zero day strategy. Arrangement will be documented to ensure availability of alternate resources. Consider sources that feature software repair factories, other project offices with similar systems and technical resources, and other contractor and vendor services.
Problem data collection	• Develop a problem resolution data collection form showing the nature of the failure, date and time of failure, when repaired, when normal operations resumed, costs associated with manual operations, and system repair/problem correction

Table 4.3 BUMIS II Zero Day Strategies

5.0 CONTINUITY OF OPERATIONS PLAN

5.1 POTENTIAL SYSTEM IMPACTS AND ALTERNATIVE PROCEDURES

As part of the pre-contingency planning, an assessment was performed to identify possible Y2K impacts to the functionality of the system. The impacts with there alternative procedure are listed below.

- BUPERS may not be able to send or receive updates due to critical failures in their system or network.

  Solution: The system will run with the most current BUPERS data. The updates to BUPERS will be archived until they can receive the data.

- The network infrastructure at BUMED ceases to function.

  Solution: A network hub and spare cables will be set up near the system. The system can operate in a limited mode until network connectivity at large is restored. If the outage is expected to continue more that several days, a modem will be used to provide access via the contractor's Internet connection.

- DOD Internet connections cease to function.

  ***Solution*:** For data being sent to BUPERS, the BUMIS II system creates files which can be archived onto floppy disks.

  The BUPERS data being sent to BUMIS II, updates are not critical to BUMIS II functionality, and can be deferred till connectivity is restored. Alternatively, BUPERS can archive the data on floppy disk, and overnight the information for input to BUMIS II. The data can be extracted from the archive floppies, placed in the proper directory, and the BUMIS II import procedures manually triggered.

5.2 CONTINUITY OF OPERATIONS PROCEDURES

This COOP provides operational level details to the BUMIS II user community. It identifies the trigger and the action that the user should initiate if they encounter a Y2K problem. A risk assessment was conducted to determine the probability of a risk occurring (P^o) and the consequence (C^o) of that risk should it occur. The risk classification (RC) is determined by multiplying P^o times C^o.

Risk/Trigger	P^o	C^o	RC	Contingency Execution	Procedures for Operating in Contingency Mode	Procedures for Returning to Normal Automated Operating Mode
System:						
1. Total system failure	L	L	L	• Report problem. • Implement manual procedures. • Determine cause, if capable, and communicate cause and/or symptoms to BUMIS II Help Desk.	• Operate in manual and/or alternate automated mode as planned. • Provide facility-wide written notification of alternate operating procedures. • Augment staff as planned. • Implement alternate data collection methods. • (Training and testing accomplished in CY99).	• Site loads new software version and conducts tests as indicated. • Facility-wide notification, date and time to resume automated operations. • Adhere to BUMIS II Project Office instructions. • Recover/reinstate data collected during manual (alternate automated) operations as directed by the BUMIS II Project Office.
2. Interface not functional	L	L	L	• Report problem. • Site cause analysis. • Implement alternate manual/automated procedures.	• Implement manual and/or alternate automated procedures for data exchange. • Provide facility-wide written notification of manual operating procedures.	• Site testing. • Facility-wide written notification that interface is active (as needed).
3. Limited/partial loss of system functionality	M	L	L	• Report problem. • Cause analysis. • Implement contingency (or alternate automated procedures.	• Begin manual and/or alternate automated procedures. • Provide facility-wide written notification. • Augment staff. • Collect data as planned.	• Site testing, as directed. • Written notification of normal operations, as needed. • Restore data, as needed.

Risk/Trigger	P^o	C^o	RC	Contingency Execution	Procedures for Operating in Contingency Mode	Procedures for Returning to Normal Automated Operating Mode
4. System-wide degraded performance or excessive system delays	M	L	L	• Report problem. • Site cause analysis. • Implement manual and/or automated contingency procedures.	• Operate system in degraded mode, as required based on extent and nature of system problem. • Provide internal notification as needed.	• Site testing, as directed. • Written notification, as required.
5. Date data (or other data) corrupted	L	L	L	• Report problem. • Site cause analysis. • Implement manual and/or automated contingency procedures.	• Operate system in degraded mode or turn system off as directed by BUMIS II Project Office or BUMED. • Operate using manual and/or alternate automated procedures.	• Site testing, as directed. • Return to normal operations IAW AIS project office instructions. • Recover/reinstate data collected during manual or alternate automated operations as directed by the BUMIS II Project Office.
6. System Print or similar function does not work	L	L	L	• Report problem. • Site cause analysis. • Operate in degraded mode. • Execute contingency procedures.	• Implement alternate manual procedures.	• Implement and test software fix.
7. Local area communications failure	L	M	M	• Report problem. • Site cause analysis. • Implement workaround contingencies.	• Implement alternate data exchange procedures. • Written notification to MID.	• Test and implement fix.
8. Wide area communications failure	L	M	M	• Report problem. • Cause/condition analysis. • Initiate contingency operations.	• Implement alternate data exchange procedures.	• Test and implement communications fix.
9. System software failure	L	L	L	• Report problem. • Cause/condition analysis. • Implement contingencies.	• Implement alternative operating procedures depending on the nature and extent of the problem.	• Test and implement system repair.

Table 5-2 Y2K Continuity Of Operations Plan

5.3 POINTS OF CONTACTS

NMIMC, Bethesda Resources Department Head
CDR Banks-Tarr
Naval Medical Information Management Center (Code 42)
8901 Wisconsin Avenue
Bethesda, MD 20889-5066
DSN: 285-1109
Com: (301) 319-1109
FAX: (301) 295-0042
Email: sbanks-tarr@us.med.navy.mil

Project Manager
Mr. Anthony Long
Naval Medical Information Management Center
8901 Wisconsin Avenue
Bethesda, MD 20889-5066
DSN: 285-1120
Com: (301) 319-1120
FAX: (301) 295-0042
Email: aflong@us.med.navy.mil

Contractor POC
Mr. Rick Hansen
Arctic Systems Inc.
15320 Spencerville Ct. Suite 201
Burtonsville, MD 20866
Com: (301) 384-8400 x101
FAX: (301) 384-6677
Email: rhansen@arctic.com

APPENDIX A. ACRONYMS AND ABBREVIATIONS

AMD	Activity Manning Document
AIS	Automated Information Systems
ASCII	American Standard Code for Information Interchange
BUMED	Bureau of Medicine and Surgery
BUMIS	Bureau of Medicine and Surgery Information System
C^o	Consequence of Risk
CA	Computer Associates
CINC	Commander In Chief
CONUS	Continental United States
COOP	Continuity Of Operations (Plan)
COTS	Commercial-Off-The-Shelf
CY	Calendar Year
DCPS	Defense Civilian Pay System
Dept	Department
DIT	Development Integration Testing
DMHRS	Defense Management Human Resources System
DoD	Department Of Defense
DOS	Disk Operating System
DTF	Dental Treatment Facilities
E-mail	Electronic Mail
EAS	Expense Assignment System
ET	Education and Training
FTE	Full-time Equivalent
FTP	File Transfer Protocol
FY	Fiscal Year
HA	Health Affairs
HD	Hard Drive
HSO	Healthcare Support Office
HTML	Hyper-Text Markup Language
H/W	Hardware
ID	Identification
IV&V	Independent Validation and Verification
JCAHO	Joint Commission on the Accreditation of Healthcare
JON	Job Order Number
LAN	Local Area Network
MB	Megabyte
MEPRS	Medical Expense and Performance Reporting System
MHS	Military Health System
MID	Management Information Department
Mil Pers	Military Personnel

NMIMC	Naval Medical Information Management Center
OASD(HA)	Office Of The Assistant Secretary Of Defense for Health Affairs
OCONUS	Outside The Continental United States
OP	Operating
ORG	Organization
OS	Operating System
OSD	Office Of The Secretary Of Defense
P^o	Probability of a risk occurring
P3	Primevera
PC	Personal Computer
PM	Program Manager
POC	Point of Contact
POMI	Plans, Operations, Medical Intelligence
R-Status	Readiness Status
RAM	Random Access Memory
RBA	Resource Business Area
RC	Risk Classification
SIT	System Integration Testing
SW	Software
WAN	Wide Area Network
WWW	World Wide Web
Y2K	Year 2000